Army in Europe Bulletin

Number 6 **HQ USAREUR/7A, Unit 29351, APO AE 09014-9351** **15 March 2003**

This bulletin expires 1 year from date of publication.

AKO ACCOUNTS FOR FAMILY MEMBERS

Army Knowledge Online (AKO) at *https://www.us.army.mil* is the Army's worldwide Intranet and is accessible from any Internet connection. All Department of the Army civilians and active duty Army, Army Reserve, and Army National Guard soldiers have AKO accounts.

Family members are authorized to establish AKO guest accounts and may use AKO's free, web-based e-mail system. This e-mail system provides an excellent means for family members to communicate with their sponsor if the sponsor deploys. AKO also allows account-holders to chat on-line and post photographs or other personal information in a secure, individual knowledge center that only the sponsor and family member can access.

To register for an AKO guest account, the family member must go to *https://www.us.army.mil*, select *I'm A New User*, and click on the *Next* button next to guest accounts. On the next screen, the family member must enter the sponsor's AKO e-mail address in the *Army Sponsor* box (sponsor's username@us.army.mil), provide the other information requested, and click on *Next*. The family member will be assigned an AKO user name and will be prompted to create a password. The password must have at least eight characters and include at least one letter and two numbers or special characters. Click on *Finish*.

An e-mail message will be sent to the family member's sponsor requesting authorization to grant the account. The sponsor must log on to his or her AKO account and enter the *Sponsor Management Console* located under the *My Army Portal* section on the AKO Homepage to authorize the account.

NOTE: Guest accounts must be renewed each year.

DSN SWITCH UPGRADE

A Defense Switched Network (DSN) switch upgrade at the Germersheim Army Depot will cause some telephone numbers with "378" prefixes to be temporarily out of service the evening of 20 March 2003.

Telephone technicians will place a new telephone switch in operation on this date after normal duty hours. Telephone numbers will not be changed.

The new telephone switch, which is operated by the Heidelberg Network Service Center, 43d Signal Battalion, is called Electronic *Wähl* (dial) System Digital (EWSD). This system uses the latest technology and will provide DSN customers with state-of-the-art, digital and analog voice connectivity.

Customers may experience short interruptions of telephone service during the switch upgrade. Emergency telephone numbers will be restored immediately. Customers who have trouble making calls after the switch upgrade should dial DSN 119 to report the problem. The 43d Signal Battalion will have technicians standing by to help customers.

The Heidelberg Network Service Center will also activate associated remote switches as follows:

Nachrichten Kaserne	11-13 April
Schwetzingen (including Kilbourne Kaserne and Tompkins Barracks)	24 April

Personnel who need more information may contact the Heidelberg Network Service Center at DSN 370-1640.

MORALE CALLS BY DEPLOYED PERSONNEL

The Department of the Army authorizes soldiers and DOD civilians deployed in remote or isolated locations for extended periods to make morale calls to their relatives and loved ones.

Current policy permits morale calls through a Defense Switched Network (DSN) operator to a local civilian telephone. This policy was recently modified by USEUCOM to allow morale calls to be made to cell phones when calling a regular telephone is not possible. In addition, if DSN operators are not available to place morale calls during the authorized times (for example, from 1701 to 0659), DSN operators at other installations who have been designated to provide service to certain locations may now place calls outside their local calling area.

Morale calls made under these guidelines will be limited to two 15-minute calls per week and only during off-duty hours. Commanders will establish controls to ensure that this privilege is not abused. This policy will be incorporated into an Army in Europe publication in the near future.

TACTICAL WHEELED VEHICLE FLEET AND THE AOAP

The United States Army Tank-Automotive and Armament Command (TACOM) recently took steps to extend Army Oil Analysis Program (AOAP) sampling intervals for tactical wheeled vehicle engines and transmissions, and to disenroll obsolete components and systems. The following new sampling intervals apply to active Army, Reserve, and National Guard units:

➢Engines will be sampled every 3,000 miles or 6 months, whichever comes first.

➢Transmissions will be sampled every 6,000 miles or 12 months, whichever comes first.

➢Hydraulic systems will be sampled each year.

A complete, detailed list of the new sampling intervals is available at *http://www.logsa.army.mil*.
NOTE: The Logistics Supply Activity (LOGSA), United States Army Materiel Command, website at *http://weblog.logsa.army.mil/aoap/openpg.htm* includes an electronic version of AOAP enrollment tables and all applicable regulations and technical bulletins.

Supported customers in the Army in Europe should not change to the new sampling intervals until LOGSA has updated the OASIS AOAP software and incorporated the sampling intervals. Once LOGSA has updated software, "DATE NEXT SAMPLE DUE" will appear on unit printouts distributed by the AOAP Laboratory. Units will then have the effective dates for the beginning the new sampling interval, which will help minimize delays and delinquencies.

Users should review the list of new sampling intervals and implement the new AOAP sampling guidance as it applies to their equipment. Local TACOM logistics assistance representatives (LARs) should be contacted for assistance. The European TACOM Office (DSN 375-3461 or civ (0049) (0)621-487-3461) has TACOM LAR names and telephone numbers.

The POC is Mr. Klosowsky at DSN 370-9104, civilian (0049) (0)6221-57-9104, or e-mail: richard.klosowsky@hq.hqusareur.army.mil.

NEW ELECTRONIC ARMY IN EUROPE PUBLICATIONS

The following Army in Europe (AE) publications have been published and are available in electronic format in the Library of Army in Europe Publications and Forms at *https://www.aeaim.hqusareur.army.mil/library/home.htm*:

➢AE Regulation 25-35, Preparing Army in Europe Publications, 26 February 2003

➢AE Regulation 525-50, Arms Control Compliance, 11 March 2003

➢AE Regulation 600-55, Driver- and Operator-Standardization Program, 25 February 2003

➢AE Regulation 614-3, Enlisted Distribution Policy, 7 March 2003

➢AE Regulation 690-81, Canteens for Local National Personnel, 18 February 2003

➢AE Regulation 690-81-G, *Kantinenbetrieb für ortsansässige Arbeitnehmer*, 18 February 2003

➢AE Regulation 840-10, Display and Presentation of U.S. Flags, 13 February 2003

➢AE Circular 190-24, Consolidated List of Off-Limits Areas, Establishments, Firms, Individuals, and Organizations, 27 February 2003

➢AE Pamphlet 190-101, Security-Threat Groups, 11 March 2003

➢AE Pamphlet 380-40, Communications Security Custodian Guide, 7 March 2003

NEW ARMY IN EUROPE COMMAND MEMORANDUMS

The following Army in Europe command memorandums have been distributed as shown:

➢Civilian Drug-Testing Program, SFIM-EU-ZS (DSN 370-7552), 14 February 2003

➢Installation Access Control System Implementation, AEAPR-PA-PL (DSN 375-2540), 18 February 2003

➢Risk-Assessment Tools for Preventing Accidents, AEAGA-S (DSN 370-8124), 5 March 2003

➢Guidance for USAREUR Leaders on Training Holidays, AEAGS-SA (DSN 377-4320), 8 March 2003

Units included in the distribution should have received their copies. Proponent telephone numbers are listed after the office symbols. These memorandums are also available in the Library of Army in Europe Publications and Forms at *https://www.aeaim.hqusareur.army.mil/library/home.htm.*

NEW ARMY IN EUROPE COMMAND POLICY LETTER

The following Army in Europe command policy letter has been distributed as shown:

➢Army in Europe Command Policy Letter 14, Company Commander/First Sergeant Course, AEAGC-TD (DSN 370-6348), 14 March 2003 (Distr: A)

Units included in the distribution should have received their copies. The proponent telephone number is listed after the office symbol. This policy letter is also available in the Library of Army in Europe Publications and Forms at *https://www.aeaim.hqusareur.army.mil/library/home.htm*.

AEPUBS

The name of the USAREUR Publications System (UPUBS) has been changed to the Army Europe Publishing System (AEPUBS).

AEPUBS is the only means of distributing Army in Europe (AE) publications. Army units in the European region will use the AEPUBS website at *https://aepubs.army.mil* to access and order Army and AE publications and forms.

AEPUBS centralizes AE publications and forms management and is maintenance-free, deployable, and easy to use. It also provides account holders complete one-stop publications service on-line.

USAREUR COMMAND POLICY LETTER RESCISSIONS

The following USAREUR command policy letters are rescinded (proponent staff offices at HQ USAREUR/7A are shown in parentheses):

➢USAREUR Command Policy Letter 1, USAREUR Training Philosophy, 20 November 2001 (Office of the G3)

➢USAREUR Command Policy Letter 2, Leadership and Force Readiness, 6 November 2001 (Office of the G1)

➢USAREUR Command Policy Letter 6, Personnel Accountability, 6 November 2001 (Office of the G1)

➢USAREUR Command Policy Letter 7, Company Commanders Training, 6 November 2001 (Office of the G3)

➢USAREUR Command Policy Letter 22, Interviewing Officers Who Decline Lieutenant Colonel and Colonel Command, 6 November 2001 (Office of the G1)

➢USAREUR Command Policy Letter 24, Command Inspection Program, 19 November 2001 (OIG)

➢USAREUR Command Policy Letter 28, Accommodating Religious Needs, 6 November 2001 (OCH)

USAREUR COMMAND MEMORANDUM RESCISSION

The following USAREUR command memorandum is rescinded:

➢Memorandum, HQ USAREUR/7A, AEAIM-P, subject: USAREUR Command Policy Letters, 25 November 2001

NEW USAPDCE TELEPHONE NUMBERS

The United States Army Publications Distribution Center, Europe (USAPDCE), has moved from Frankfurt, Germany, to the Mannheim area. New USAPDCE numbers are as follows:

Director	384-6890
Customer Support	384-6898/6893
Inventory Management	384-6891/6892
Automation Division	384-6897/6896
fax	384-6111/6894

ARMY IN EUROPE IA POLICY

The integrity of automation systems in the Army in Europe must be preserved. Information assurance (IA) protects automation systems and data, whether installed on or passed through the system. Safeguarding both systems and data is a nonnegotiable responsibility. Appendix A provides the IA policy for the Army in Europe.

HOW TO USE THIS BULLETIN

HQ USAREUR/7A and the United States Army Installation Management Agency, Europe Region Office (IMA-Europe), publish the Army in Europe Bulletin on the 1st and 15th of each month.

Only personnel assigned to HQ USAREUR/7A staff offices or IMA-Europe may publish articles in the bulletin. Personnel assigned to USAREUR major subordinate and tenant commands may also submit items, provided the request is sent through the command's affiliated HQ USAREUR/7A staff office. Personnel assigned to area support groups and base support battalions may also submit items for publication in the bulletin, provided the request is sent through a division of IMA-Europe. Requests may be sent by fax (DSN 370-6568), mail (USAREUR G6 (AEAIM-P), Unit 29351, APO AE 09014-9351), or e-mail (pubsmail@hq.hqusareur.army.mil).

Personnel who would like to receive the bulletin may subscribe to have it delivered directly to their e-mail accounts by registering through the Personal Subscription Notification (PSN) feature in the Army in Europe Publishing System at *https://aepubs.army.mil* (click on "PSN").

Personnel with questions or comments about this bulletin may contact the bulletin editor by telephone (DSN 370-6755) or e-mail (pubsmail@hq.hqusareur.army.mil).

For the CG, USAREUR/7A:

ANTHONY R. JONES
Major General, GS
Chief of Staff

Official:

GARY C. MILLER
Regional Chief Information Officer - Europe

DISTRIBUTION:

This bulletin is distributed by e-mail and is available only in electronic format.

APPENDIX A
ARMY IN EUROPE INFORMATION ASSURANCE POLICY

COMPUTER-USER TEST

The Computer-User Test Program requires all personnel to take a computer-user test if assigned to an organization that is connected to the Army Nonsecure Internet Protocol Router Network (ANIPRNET) or the Army Secret Internet Protocol Router Network (ASIPRNET). This policy applies to all categories of employees, including military, DA civilian, contractor, and local national (LN) personnel. (The Head Works Council, USAREUR, concurs with this policy.) All computer users in the Army in Europe must comply with this policy before being issued a network password or user identification.

The computer-user test is available in English and German on the USAREUR Automation Training Program Webpage at *https://www.uatp.hqusareur.army.mil*. The test is open-book, multiple-choice, self-paced, and user-friendly. Users may take the test at their desks. The test must be taken every 3 years.

Before taking the test, personnel should read the Army in Europe Computer-User Guide. This study guide is available in English and German. The USAREUR Automation Training Program Webpage provides links to the on-line versions of these study guides.

In addition to taking the test, computer users must print out the Computer-User Agreement from the webpage and sign it. LN employees in Germany should sign the German version of this agreement. Unit system administrators will keep signed agreements in their files.

The USAREUR Automation Training Program Webpage provides more information on the Computer-User Test Program.

ARMY IN EUROPE POLICY ON ASSIGNING COMPUTER-USER ACCOUNTS TO FOREIGN COALITION FORCES AND FOREIGN-NATIONAL CONTRACTORS

Among the personnel using computers and computer networks in the Army in Europe are local national employees of the U.S. Government, foreign-national representatives to the U.S. Government, and foreign-national contractors. The policy below applies only to foreign-national representatives to the U.S. Government and foreign-national contractors.

Foreign-national representatives of Allied or coalition partner countries (both NATO and non-NATO) and foreign-national contractors—

- May be provided limited-access user accounts on unclassified computer networks in the Army in Europe if approval is granted by the Joint Chiefs of Staff and the DAA.

- Must sign a computer-user agreement before being given an account.

- May use accounts only for communicating with the U.S. coalition command structure under which they fall. This use must be consistent with the mission of the coalition command and with the guidance issued by the U.S. commander responsible for the computer network.

If a computer or computer network is to be used by foreign-national representatives or contractors, official DOD information on the computer or computer network that pertains to military matters and national security issues must be reviewed for clearance according to DOD Directive 5230.9.

E-mail addresses of foreign-national representatives and contractors must include information that identifies the account-holder's country.

- The full country name must be included in the e-mail alias. The alias format must be "name, country, duty description."

- Simple mail transfer protocol (SMTP) addresses must include the two-letter Federal Information Processing Standard (FIPS) 10-4 codes for country designations (for example, name.FIPScountrycode@C/S/A.mil).

Examples of the proper format for aliases and e-mail addresses are as follows:

Alias: John Doe, Australia, LNO, CINC
SMTP: john.doe.as@cinc.mil

Alias: John Smith, United Kingdom, FLO, Service
SMTP: john.smith.uk@service.mil

- E-mail auto-signature blocks must include foreign individual's name, nationality, duty description, and organization assigned. For example:

John Doe, WG CDR
United Kingdom - FLO
CINC, J6

Computer networks that will be used by foreign-national representatives and contractors will be configured to provide only the minimum Internet access required for the mission.

Policy on the appropriate use of computer networks in the Army in Europe and on limited personal use of U.S. Government computers also applies to foreign-national representatives and contractors. Those who misuse computer networks in the Army in Europe will lose access to them, and financial reimbursement for any monetary liability will be requested from the sending country if permitted by applicable international agreements.

ARMY IN EUROPE POLICY ON BLACKBERRY PERSONAL ELECTRONIC DEVICES (PEDS)

The BlackBerry personal electronic device (PED) is a popular information technology tool that allows for wireless voice and data transmission. Information transmitted through a PED, however, does not remain completely within DOD networks; it is communicated through and stored on a foreign, non-Government message center, and is therefore vulnerable to unauthorized access. Because of this vulnerability, use of BlackBerry PEDs to process and transmit official Government information, including For Official Use Only (FOUO) information, is prohibited for the Army in Europe.

An enhanced U.S.-Government version of BlackBerry is being tested and may be authorized for use in the future.

ARMY IN EUROPE POLICY ON BLOCKING HIGH-RISK E-MAIL ATTACHMENTS

As part of the ongoing server consolidation effort, USAREUR is migrating toward a theater-managed policy to block e-mail attachments that have high-risk file extensions.

Many viruses circulating today are sent as attachments to e-mail messages. Hackers often transmit known viruses or develop new ones using files with the extensions listed in the following table. Units can help protect our networks by blocking e-mail attachments that have high-risk file extensions. In addition, since anti-virus software always lags behind the identification of a new virus, our networks will already be protected against many new viruses by blocking these e-mail attachments.

System administrators will configure their exchange servers to quarantine e-mail attachments that have the file extensions listed in the following table. Local designated approving authorities (DAAs) may grant an exception to this list within their portion of the network.

The USAREUR Information Assurance Program Manager will update the exchange computer-security baseline to include this requirement and will institute a theater-level blocking capability to protect against immediate and future threats.

File Extension	File Type
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML help file
.cmd	Microsoft Windows NT command script
.com	Microsoft MS-DOS program
.cpl	Control panel extension
.crt	Security certificate
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup information
.ins	Internet naming service
.isp	Internet communication settings
.js	JScript file
.jse	JScript encoded script file
.lnk	Shortcut
.mde	Microsoft Access MDE database
.mp3	File sharing
.msc	Microsoft common console document
.msi	Microsoft Windows installer package
.msp	Windows installer patch
.mst	Visual test source file
.pcd	Microsoft visual test compiled script or photo CD image
.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen saver
.sct	Windows script component
.shb	Shortcut into a document
.shs	Shell scrap object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript encoded script file
.vbs	VBScript file
.wsc	Windows script component
.wsf	Windows script file
.wsh	Windows script host settings file

ARMY IN EUROPE POLICY ON COALITION NETWORKS

Computer networks established for combined (coalition) joint task force missions should operate at security and access levels that will best support the personnel involved in the missions.

A coalition Secret network, in which foreign-national representatives in the coalition are provided information by "air gap" (transferring information from one system to another by using a diskette or compact disk), is the most useful computer-network architecture for joint task forces. Combined task force operations centers that use coalition Secret networks avoid the problems that arise from using U.S. Only Secret networks, to which foreign-national representatives do not have access. U.S. Only Secret networks may also be connected with coalition Secret and unclassified networks using the Secret and Below Interoperability (SABI) process.

Most information on coalition networks pertains to the coalition and may be shared with foreign-national representatives based on a mission-driven "need to know." National information that supports multinational efforts may be shared based on national rules. U.S. personnel who share U.S. national information must follow National Disclosure Policy (AR 380-10).

Information provided to coalition networks must pass through U.S. national intelligence centers (NICs). A designated foreign disclosure officer or a U.S. NIC may be established as the authorized terminus for classified and unclassified U.S.-only computer networks and other telecommunications traffic.

Under no circumstances will non-U.S. citizens be—

➢Given a computer-user account on any U.S. classified network for any reason.

➢Assigned to work in any area (office, tent, open bay) where U.S. Only classified information is being processed.

SABI Process
The SABI process—

➢Was designed to interconnect Secret and unclassified networks.

➢Follows the four phases of the DOD Information Technology Security Certification and Accreditation Process (DITSCAP).

➢Requires that all interconnected networks be fully certified and accredited and that all associated security devices be certified, tested, and evaluated according to the partnership-compliance standards of the National Security Agency and the National Information Assurance Partnership.

DOD organizations must use the SABI process when connecting networks of different classification levels. Army organizations will do the following:

➢Submit mission-requirement and proposed security-architecture documents through their chain of command to the Army CIO/G6 (SAIS-IAS) for concept review.

➢Coordinate with the Communications Security Logistics Activity (CSLA) for acquisition of guards and Type 1 encryption devices. Organizations will submit their requirements through their information assurance manager (IAM). IAMs will enter requirements in the CSLA Information Systems Security Program database at *https://issp.army.mil*.

➢Once the CIO/G6 and the CSLA have reviewed and accepted the plan, go to the SABI Information Homepage at *http://www.sabi.org*, complete a SABI ticket submittal form, and request a SABI starter kit.

NOTE: Army organizations that want to acquire security devices that are not on the list of products approved by the Defense Information Systems Agency (DISA) should consider the extended timeline and associated certification costs before attempting to begin the SABI process.

Interconnections of DOD information systems will be managed constantly to minimize risk by ensuring that the assurance of one system is not adversely affected by vulnerabilities of other interconnected systems.

Army organizations that maintain connections between networks of different classification levels must revalidate their connection each year according to Secret Internet Protocol Router Network (SIPRNET) designated approving authority directives.

Units may obtain information on current guidance and requirements from the DISA at *https://iase.disa.mil/cap/index.html*.

ARMY IN EUROPE POLICY ON COMMERCIAL INTERNET CHAT

Army Knowledge Online (AKO) provides an Internet chat tool for Army users. This tool is the only authorized chat tool for the Army Nonsecure Internet Protocol Router Network (ANIPRNET).

Commercial Internet-chat tools present an unacceptable risk to the integrity, availability, and confidentiality of our data and data networks. Tools such as the America Online (AOL) Instant Messenger, ICQ, mIRC/IRC, SPiN Chat, Yahoo Chat, and websites that promote chat services are unauthorized for use on the ANIPRNET.

Certain chat tools are authorized on the Army Secret Internet Protocol Router Network (ASIPRNET). These tools are documented in the system security authorization agreement for the specific application that uses them.

ARMY IN EUROPE POLICY ON COMPUTER ANTI-VIRUS PROTECTION

Virus attacks on computer networks worldwide are becoming more frequent and more destructive. To limit vulnerability to these attacks, anti-virus signatures on all Government computers (GCs) (desktops, laptops, and personal electronic devices (PEDs) (such as personal digital assistants (PDAs))) in the Army in Europe must be updated weekly. Anti-virus signatures on all file servers will be updated daily.

An automatic daily update pushed to individual users (automatically placed on their systems) is the preferred method for updating anti-virus signatures on GCs. When automatic daily updates are not available, GC users are responsible for updating anti-virus signatures on their GCs.

This policy applies to both classified and unclassified computer networks, but not to Uniplexed Information and Computer Systems (UNIX) or other non-Microsoft operating systems that are less vulnerable to virus attacks.

Only the DOD-licensed Norton, McAfee, and TrendMicro anti-virus software products are authorized for use in the Army in Europe. The DOD site license provides Norton, McAfee, and TrendMicro anti-virus software free of charge to Army computer users. The use of any other product requires a waiver endorsed by the USAREUR Information Assurance Program Manager and approved by the Army CIO/G6. Waivers will not be granted without clear, strong, mission-related justification for using another anti-virus product.

The DOD site license allows DOD employees to use Norton, McAfee and TrendMicro anti-virus software on their home computers and or PEDs/PDAs. Contractors may not use these products on personal home computers, but may load it on company computers used for executing DOD contracts. Current anti-virus products are available on the USAREUR iAssure Website at *https://iassure.usareur.army.mil* and the DOD CERT Website at *http://www.cert.mil*. Users must have a ".mil" Internet protocol (IP) address to download these products. File downloads from these websites may be made to individual floppy disks, or one large file may be written to a diskette using a CD-ROM burner.

The DOD site license now extends its contracts to offer anti-virus software for PEDs, such as PDAs, handheld computers, and similar devices. Individual commands are responsible for obtaining anti-virus software for these devices, if none are available under the site license for a particular brand or operating system.

Users who suspect that their GC has been infected with a virus or malicious logic, or who observe unusual or suspicious behavior on their GC, should do the following:

- Leave the computer on.
- Disconnect the network cable from the computer.
- Report the incident to their supervisor and local system administrator.

Personnel who need anti-virus software assistance may contact their local network services center or go to the USAREUR iAssure Website at *https://iassure.usareur.army.mil* or the DOD CERT Website at *http://www.cert.mil* to download tips and installation guides.

ARMY IN EUROPE POLICY ON COMPUTER NETWORK MINIMIZE

Periods of increased military operating tempo (OPTEMPO) place a higher demand on our limited computer network capacity. This increased demand slows the network, which can affect mission accomplishment.

To ensure the network capacity can support our mission, the Office of the G3, HQ USAREUR/7A, may issue Network MINIMIZE messages during periods of increased OPTEMPO. These messages will remain in effect until they are rescinded by another USAREUR G3 message.

Network MINIMIZE applies only to networks in the Army in Europe. When Network MINIMIZE is announced, units must limit their network use, particularly during peak hours (0700 to 1900 Central European Time).

Examples of measures that may go in effect during Network MINIMIZE include, but are not limited to—

- Applying operations-security restrictions on the content of e-mail messages that will be sent outside the command.
- Establishing approval authorities for e-mail messages that will be sent outside the command.

➢Placing restrictions on—

•Personal use of Government computers (GCs) and networks.

•The size of e-mail messages and attached files.

•The use of global addresses.

•The use of mission-related streaming audio and video.

During Network MINIMIZE, mission-essential communications, which include reasonable use of GCs and networks for morale and educational purposes, will be maintained. Personal use of GCs will not be permitted except for the following:

➢Limited morale e-mail by soldiers, civilian employees, and DOD contractors in the central region of USAREUR operations.

➢Limited morale e-mail by soldiers, civilian employees, and DOD contractors in the forward area of USAREUR operations (Bosnia and Herzegovina, Kosovo, Macedonia, and other contingency locations).

➢Use of unit computers by family-support groups to communicate with family members downrange, according to the time limits in the above two categories.

➢Minimum-essential use of computers at Army education centers for educational purposes. This use will be restricted to off-duty hours. Faculty supervision is requested.

➢Minimum-essential use of unit computers for educational purposes. This use will be restricted to off-duty hours and requires supervisory (GS-13, lieutenant colonel, or above) approval.

➢Use of GCs that are not connected to Government networks.

Network MINIMIZE messages will provide provisions for obtaining waivers to restrictions on network use.

ARMY IN EUROPE POLICY ON COMPUTER-NETWORK MISBEHAVIOR

Commanders and supervisors, with help from their information technology and information assurance staff, are responsible for the discipline of the users and operators of USAREUR computer networks. The information technology and information assurance staff includes the senior signal staff officer, the information management officer (IMO), system administrators (SAs), network administrators (NAs), information assurance managers (IAMs), and information assurance security officers (IASOs). DOD Regulation 5500.7-R (Joint Ethics Regulation) and DA and Army in Europe policy define computer-network misbehavior.

Prohibited Activities
Prohibited computer-network activities include the following:

➢Having or loading prohibited software onto GCs. Prohibited software includes peer-to-peer file-sharing software, such as MP3 music and video software; streaming audio and video; hacker tools and development software; malicious logic and virus-development software, executables (files with an ".exe" extension), and macros; network line-monitoring and key-stroke-monitoring tools; unlicensed (pirated) software; web-page-altering software; games (including "America's Army"); personal firewalls (including DOD-licensed firewalls and Windows XP Internet connection firewalls (ICFs)); and any software not authorized by the unit commander and IMO.

➢Using a commercial internet-chat tool such as America Online (AOL) Instant Messenger, Yahoo Chat, and websites that promote chat services. Army Knowledge Online (AKO) is the only authorized chat service allowed on the Army Non-secure Internet Protocol Router Network (ANIPRNET).

➢Using networked information technology or GCs for personal gain or illegal activities.

➢Releasing, disclosing, or altering information without the consent of the data-owner, the original classification authority as defined by AR 380-5, or the individual's supervisory chain of command; or the approval of the Freedom of Information Act officer, public affairs officer, or foreign-disclosure officer.

➢Attempting to strain, test, circumvent, or bypass security mechanisms, or performing network line-monitoring or key-stroke-monitoring without proper authorization. Use of web-anonymizer services from the ANIPRNET is considered bypassing security mechanisms and is prohibited.

➢Modifying system equipment or software, using system equipment or software for other than its intended purpose, or adding software without SA, IASO, or IMO approval. This includes the USAREUR Computer Security Baseline. Under no circumstances will a user or SA modify the Windows XP baseline to initialize the Windows XP built-in firewall (ICF).

➢Relocating or changing information technology equipment or the network connectivity of information technology equipment without proper security authorization.

➢Introducing malicious code (for example, viruses, worms) into any information technology or network.

➢Sharing user-identification or passwords.

➢Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene material. This material includes but is not limited to "hate literature," such as racist literature, material, or symbols (for example, swastikas and other neo-Nazi material), and sexually harassing material. Obscene material includes but is not limited to pornography and other sexually explicit items.

➢Storing or processing classified information on a system not approved for classified processing.

➢Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

➢Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

➢Using another person's account or identity without appropriate authorization or permission.

➢Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

➢Giving an unauthorized individual access to a Government-owned or Government-operated system.

➢Hacking the USAREUR network.

➢Sending or forwarding official e-mail from a computer connected to the ANIPRNET through a commercial Internet service provider (ISP) (for example, America Online, CompuServe, Hotmail, Yahoo) to another commercial e-mail account or to another .mil address.

➢Using someone else's user identification and password or masking or hiding your identity.

➢Installing and using a modem without approval from the designated approval authority.

➢Writing or forwarding chain or hoax e-mail messages.

➢Posting personal homepages.

➢Downloading or loading Freeware or Shareware software.

➢Simultaneously connecting to a Government network and a commercial ISP using a modem or virtual private network (VPN) connection from your GC, personal digital assistant (PDA), or personal electronic device (PED).

COMMANDER AND SUPERVISOR ACTIONS

Soldiers or civilians suspected of engaging in prohibited computer-network activities will—

➢Be suspended immediately from network access pending the results of a commander's inquiry.

➢Have their computer accounts inactivated for the duration of the commander's inquiry. Passwords that these individuals know will be changed immediately.

➢Be ordered not to use any Government computer or network pending the results of the commander's inquiry.

Soldiers who fail to comply with this policy may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). Personnel not subject to the UCMJ may be subject to adverse action under the United States Code or Code of Federal Regulations.

ASSESSING DAMAGE

The Army Network Operations and Security Center, Europe (ANOSC-Eur), the Regional Computer Emergency Response Team, Europe (RCERT-E), and the 202d Military Police Group will provide technical assistance as required to help commanders assess damage caused by the suspected computer-network misbehavior.

The ANOSC-Eur and RCERT-E will—

➢Assess damage that may have resulted from the suspected violator's activities, particularly as they relate to the ANIPRNET and Army Secret Internet Protocol Router Network (ASIPRNET).

➢Report any damage or harmful activity outside the ANIPRNET.

Computer forensic specialists from the 202d Military Police Group will examine the computer hard drive and other components for evidence of the suspected activity. RCERT-E personnel also will examine RCERT-E computer-activity logs.

PRESERVING EVIDENCE

Computer forensic specialists will remove computers involved in suspected violations from the network for examination. These computers will be treated as physical evidence of a crime until released by competent authority.

DETERMINING A COURSE OF ACTION

The unit information technology and information assurance staff, local network services centers, regional network operations and security centers, the ANOSC-Eur, RCERT-E, and the 202d Military Police Group will help unit commanders determine what violations occurred, how they happened, and what damage was caused. The commander will then determine appropriate disciplinary and administrative actions.

ARMY IN EUROPE POLICY ON INFORMATION ASSURANCE VULNERABILITY ALERTS

Information assurance is a commander's program. Direct command emphasis is needed to make it work.

GENERAL

Information assurance vulnerability alerts (IAVAs) are official notifications to the command that a software security vulnerability has been identified that affects one or more Army computer systems worldwide. These vulnerabilities are almost always public knowledge and involve commercial software products.

Known vulnerabilities are favorite targets of hackers who probe computer networks in the private and public sectors to find unprotected computers. When a command receives an IAVA, the command must quickly determine if any of its computers are affected and, if so, immediately fix them.

When HQDA issues an IAVA, the G3, USAREUR, will forward it to commands in the Army in Europe as a formal tasker. These taskers come in three forms:

➢Numbered DRAGON LIGHTNING alerts, which are issued when a clear and present danger threatens the integrity, confidentiality, or availability of our data and networks, which in turn threatens our warfighting capability.

➢Numbered Army IAVAs, which are issued when the threat is not as immediate or severe, but may degrade our warfighting capability.

➢Numbered USAREUR alerts, which are specific to the Army in Europe or are not covered by an Army IAVA.

Compliance reporting for USAREUR-initiated taskers, including DRAGON LIGHTNING alerts, must be completed on the USAREUR iAssure Website at *https://iassure.usareur.army.mil/policy*. As USAREUR-initiated taskers are released, the Office of the USAREUR Information Assurance Program Manager will provide guidance. Units should contact the Office of the USAREUR Information Assurance Program Manager for a login if they do not already have one.

RESPONDING TO USAREUR IAVAS

The USAREUR iAssure Website at *https://iassure.usareur.army.mil/policy/iava/compliance.aspx* provides an IAVA Compliance Reporting Database (CRD) checklist and procedures for submitting compliance reports. Units must respond to IAVAs and submit compliance reports according to the procedures on this website. Servicing information assurance managers can also provide information on these procedures.

Responses to USAREUR IAVAs will include the following information in the IAVA CRD:

A. Number of assets affected. (For the purpose of this policy, assets are defined as the systems listed in the "Systems Affected" section of an IAVA.)

B. Number of assets in compliance.

C. The comment "closed" at level 2 in the IAVA CRD hierarchy as appropriate to indicate that the unit has closed out the IAVA.

Organizations that are unable to comply with an IAVA by the suspense must apply for an extension in writing before the compliance date. Extensions must be submitted to the Office of the USAREUR Information Assurance Program Manager using the USAREUR IAVA compliance extension form on the USAREUR iAssure Website. These organizations must also submit a "road map" for meeting the requirement with dates, and a description of the temporary security procedures that the organization will take to ensure the security of the military network. The organization DAA must sign the extension request.

SYSTEM COMPLIANCE

Before any new system is connected to a network in the Army in Europe, SAs will ensure it is in compliance with all IAVAs that pertain to it. SAs will create and locally maintain IAVA logs on servers that will list the compliance status for each system they manage. The logs will list, as a minimum, all existing IAVAs, patches, upgrades, hot fixes, service packs, and other actions that pertain to each system and the date each action was taken. If a system is reconfigured or restored after a malfunction, the log will be used to ensure that all necessary actions are reapplied. All actions reapplied and any added will be entered in the log again.

NOTE: IAVA logs are not required for individual computer workstations.

ARMY IN EUROPE POLICY ON IT/IA WORKFORCE TRAINING

TRAINING AND TESTING

A trained information technology/information assurance (IT/IA) workforce is the foundation for secure computer networks. The Army CIO/G6 and Army in Europe policy require special training for system administrators, network administrators and managers, IA security officers and managers, and anyone else with elevated privileges on a network server or router in the Army in Europe, regardless of their duty assignment. This policy provides a consistent baseline of computer-network security training for key professionals who operate and secure our computer networks.

All military, DA civilian, contractor, and local national personnel appointed to IT/IA workforce positions must be certified before being granted elevated privileges on a network in the Army in Europe. Personnel with elevated privileges who are in the Army in Europe on official temporary duty (TDY) for more than 60 days must attend training or pass the on-line Information Assurance/Computer Network Defense Training Program (IA/CND TP) test before assuming IT/IA duties on a network in the Army in Europe.

IA/CND TP COURSES

The USAREUR IA/CND TP provides required IA and computer network defense training at 12 locations in the European theater. This training meets all IA/CND computer-training standards mandated by HQDA. Units do not have to pay for the training, but must pay for TDY costs associated with the training.

No one will be assigned to, or continue their assignment in, the IT/IA workforce, or be given elevated privileges on any portion of a computer network in the Army in Europe unless they are certified by the Army CIO/G6 School of Technology's Information Assurance Course or have attended or are scheduled to attend the USAREUR IA/CND TP course.

IA TRAINING WEBSITES

Information on the USAREUR IA/CND TP is available at *https://www.uatp.hqusareur.army.mil*.

Personnel who need more information on IA training and related IA issues should first visit the USAREUR iAssure Website at *https://iassure.usareur.army.mil*. The following additional websites may be used as a final source of information on IA:

➢Certification and accreditation forms and templates, Army Secret Internet Protocol Router Network (ASIPRNET) documents, and ASIPRNET dial-in IA documents may be downloaded from the USAREUR iAssure Website at *https://iassure.usareur.army.mil*.

➢IA training compact disks and videotapes may be ordered free of charge from the Defense Information Systems Agency IA webpage at *http://www.disa.mil/infosec/iaweb/default.html* (click on Education and Training, then Products Order Form).

➢IA policy and guidance may be obtained from the DOD Computer Emergency Response Team website at *http://www.cert.mil*.

➢Training information may be obtained from the Fort Gordon School of Information Technology website (requires an Army Knowledge Online (AKO) account to access).

➢The United States Army Computer Emergency Response Team website at *https://www.acert.1stiocmd.army.mil/ACERTmain.htm* provides information on anti-virus software, information assurance vulnerability alerts (IAVAs), training, and briefings.

ARMY IN EUROPE POLICY ON PROHIBITED COMPUTER SOFTWARE

Software may be loaded on Government computers (GCs) only with the approval of the unit commander and the information management officer (IMO).

PROHIBITED SOFTWARE

Prohibited software includes the following:

➢Peer-to-peer file-sharing software (for example, MP3 music and video software).

➢Streaming audio.

➢Streaming video.

➢Hacker tools.

➢Malicious logic and virus-development software.

➢Malicious logic and virus executables and macros.

➢Unlicensed and unapproved shareware.

➢Network line-monitoring tools.

➢Keystroke-monitoring tools.

➢DOD-licensed personal firewalls from Symantec, McAfee and TrendMicro and Windows XP ICF firewall. Personal firewall software is authorized for home use for soldiers and DOD civilians.

NOTE: Software manufacturers should be contacted for support with their programs if needed. System administrators and network service centers should not be called for support.

➢Personal software not authorized by the unit commander and IMO.

➢Unlicensed (pirated) software.

➢Webpage-altering software, such as Aureate, Cydoor, Ezula Top Text, Gator, Limewire, and Spedia Surf+.

NOTE: This software only infects Internet Explorer.

➢Games other than officially Army sanctioned simulations. ("America's Army" is not an Army-sanctioned simulation.)

➢Any software not authorized by the unit commander and IMO.

ARMY IN EUROPE POLICY ON PASSWORDS

Secure passwords are the first line of defense against the misuse of Government computers.

Passwords must be less than 180 days old (90 days on classified systems) and must conform to the following standards:

The information assurance officer (IAO) or a designated representative in each organization will be responsible for issuing and controlling passwords. This responsibility may not be delegated. The IAO or designated representative will use one of the following two methods to issue passwords for their organizations:

➢Generate passwords at the information management office (IMO)-level and have users sign for them. If this method is used, the passwords must be random, eight-character, alphanumeric codes with at least two numbers and two letters. Passwords must not form a word.

➢Allow users to create their own passwords based on a system prompt, and use a password filter that ensures the passwords are eight characters long and include at least one uppercase character, one lowercase character, one special character, and one number. Passwords must not form a word or repeat any of the last 10 passwords created by the user.

A password creator and instructions, and a password filter and instructions, are available on the USAREUR iAssure Website as follows:

➢For the password creator*:* *https://iassure.usareur.army.mil/downloads/download_file.aspx?fileID=399*.

➢For the password filter: *https://iassure.usareur.army.mil/downloads/download_file.aspx?fileID=684*.

ARMY IN EUROPE POLICY ON INTERNET WEBSITE ACCESS LIMITS

Web-based Internet access, or websurfing, has ethical, network security, and network operation implications. DOD policy defines limits on Internet access from Government computers (GCs). The Joint Ethics Regulation, paragraph 2-301, prescribes behavior and personal use that is permitted on a limited basis. USAREUR information assurance policy defines further limits.

USAREUR has a new network tool to help enforce DOD policy on the appropriate use of the Internet and to increase the amount of network bandwidth available at key times for mission purposes. This network tool groups known websites into a series of specific categories based on content. Users will be allowed access to websites in each category, subcategory, or a group of categories either all the time or only during certain times of the day. Websites devoted to prohibited activities (for example, pornography, hacker sites, chat rooms, gambling) will be permanently blocked.

The USAREUR Information Management Council of Colonels will identify and approve a USAREUR template of blocked websites for use with this tool. This template will specify minimum categories of blocked websites and times when personal use of GCs for web browsing is not allowed.

Regional senior tactical commanders (STCs) may impose more restrictive access guidelines in their regions. Regional network operations and security centers will coordinate with STCs and implement these guidelines.

ARMY IN EUROPE POLICY ON WEBSITE SECURITY AND INFORMATION CONTENT

Organizations with websites must take steps to limit exposing webservers to risk.

PUBLIC WEBSITES

All public websites (those intended for unrestricted access) reside on servers managed by the Office of the Chief, Public Affairs (OCPA), HQ USAREUR/7A. These servers will remain accessible from Internet protocol (IP) addresses in Europe and North America. Units with public websites that, for technical reasons, cannot reside on the OCPA servers must receive approval from the USAREUR Information Assurance Program Manager.

PRIVATE WEBSITES

Private websites (those limited to a specific domain (DOD, Army, USAREUR, or other defined group)) may be hosted on organizational webservers or consolidated community servers. Security measures will be taken locally and at the network perimeter. To comply with Message, HQDA, SAIS-ZA, 101256Z May 00, subject: Public Key Enabling of Private Web Servers, all private Army webservers in the Army in Europe must operate secure socket layer (SSL) protocol using a Class 3 Public Key Certificate issued by the DOD Public Key Infrastructure (PKI). The USAREUR iAssure Webpage at *https://iassure.usareur.army.mil* provides information on implementing SSLs on private webservers.

Additional local security measures, such as password protection or limiting the range of authorized IP addresses, are at the discretion of each organization.

WEBSITE CONTENT

Because the Internet is a public forum, organizations in the Army in Europe will ensure that the commander, the public affairs officer, and other appropriate designees (for example, command counsel, force protection and intelligence offices) have properly cleared information posted to the World Wide Web. Commanders will ensure that websites are routinely reviewed quarterly to ensure that each website is in compliance with the policy outlined in AR 25-1 and that the content remains relevant and appropriate.

Information contained on publicly accessible websites is subject to the policy and clearance procedures prescribed in AR 360-1, chapter 5, for the release of information to the public. In addition, Army organizations using the World Wide Web will not put the following types of information on publicly accessible websites:

- Classified or restricted-distribution information.
- For Official Use Only (FOUO) information.
- Unclassified information that requires special handling (for example, encrypt for transmission only, limited-distribution, and scientific and technical information protected under technology transfer laws).
- Sensitive but unclassified information, such as proprietary information, predecisional documents, and information that must be protected under legal conditions such as the Privacy Act.
- Information exempt from disclosure under the Freedom of Information Act. This includes lists of names and other personally identifying information of personnel assigned to a particular component, unit, organization, or office in the Department of the Army. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties, such as general officers and senior executives, public affairs officers, or other personnel designated as official command spokespersons, is permitted.
- Draft publications. AR 25-1, paragraph 9-2, provides more information.